



Department of Homeland Security Daily Open Source Infrastructure Report for 19 July 2007

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- Counterterrorism investigators in New Jersey now have real-time access to information on potentially hazardous shipments on CSX Transportation, one of the nation's largest rail networks. (See item [17](#))
- The White House Homeland Security Council on Tuesday, July 17, released a one-year update on the federal government's pandemic influenza preparedness strategy, reporting that it has met 86 percent of the objectives it set for itself a year ago. (See item [30](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 17, U.S. Department of Energy* — **DOE and NRC increase cooperation to advance Global Nuclear Energy Partnership.** The U.S. Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) expanded cooperation for President Bush's Global Nuclear Energy Partnership (GNEP) through a Memorandum of Understanding (MOU) that was signed on Friday, July 13, by DOE's GNEP Deputy Program Manager Paul Lisowski and NRC Executive Director for Operations Luis Reyes. The MOU establishes the foundation for increased cooperation between DOE and NRC on technological research and engineering studies and marks another important milestone towards closing the nuclear fuel cycle in the

United States. Through this cooperation memorialized in the MOU, DOE will share the latest information on advanced recycling technologies with the NRC, enabling them to develop license criteria for GNEP facilities. The NRC will also participate in and observe DOE tests, simulations, and demonstrations. NRC will review and provide feedback to DOE on GNEP reports and engineering studies, review literature and take facility tours, and provide annual reports to DOE on work performed under this MOU. DOE and NRC officials agreed to continue to regularly meet and exchange the latest GNEP information.

Source: <http://www.energy.gov/news/5245.htm>

2. *July 17, Reuters* — **OPEC expects modest rise in 2008 demand.** The Organization of Petroleum Exporting Countries (OPEC) said Monday, July 16, that world oil demand in 2008 will grow moderately while supply from rival producers will expand, reducing the need for crude from the exporter group. The assessment, in OPEC's July Monthly Oil Market Report, underscores OPEC's view that crude supply is enough and oil prices near a record high reflect a strain on refineries and other factors beyond its control. OPEC said world oil demand in 2008 would rise by 1.34 million barrels per day, or 1.6 percent, slowed in part by conservation and use of other fuels.

Source: <http://archive.gulfnews.com/articles/07/07/17/10139731.html>

3. *July 17, Associated Press* — **Designed with quakes in mind, nuclear plants rarely damaged by seismic activity.** With 20 percent of the world's nuclear reactors in seismically active zones and the remote but real possibility of earthquakes just about everywhere else, nuclear power plants are designed with shaking in mind. Plants in many countries have survived quakes more powerful than the one that hit Japan on Monday, July 16, suggesting that the poor performance of the Kashiwazaki Kariwa reactor is more illustrative of recent safety problems in the country's nuclear industry than any inherent vulnerability of the technology. The U.S. Nuclear Regulatory Commission requires utilities to design nuclear plants so they can safely shut down in the event of a powerful earthquake, typically the strongest that geologists consider possible in the region. Plants are also required to be able to operate without disruption through a weaker earthquake, usually one about half as strong as the maximum. Even some of the deadliest earthquakes in recent history have produced little or no damage to nuclear reactors in the affected area. Though a December 1988 earthquake in northwestern Armenia killed 25,000 people, two Soviet-designed reactors about 50 miles from the epicenter continued to operate normally.

Source: http://www.signonsandiego.com/news/nation/20070717-1320-quak_esandnukes.html

4. *July 16, Daily News (MA)* — **Police question response from Seabrook nuclear power plant.** Three days after an emergency siren for New Hampshire's Seabrook Nuclear Power Plant malfunctioned and caused fear across large parts of Amesbury, MA, officials are questioning how the incident was handled and pledging to change plans for responding to similar problems in the future. As the alarm wailed from a single pole in Amesbury on Friday, July 13, hundreds of calls from worried residents flooded the 911 center. Some callers wondered whether they needed to immediately evacuate the area. Others tried unsuccessfully to get more information from the radio. But neither police nor the media had answers. Amesbury is one of six Massachusetts communities within a 10-mile radius of the nuclear power plant that have the warning sirens, which are affixed to poles and look like loudspeakers. The loudspeakers were not used because power plant officials believed Amesbury police officers were communicating to residents that there was no emergency, said Alan Griffith, the senior communications adviser

for the Seabrook plant. Power station officials spent Sunday, July 15, in talks with state officials, including the Massachusetts Emergency Management Agency, on plans to make sure the best communication is in place to make the public feel safe, Griffith said.

Source: http://www.newburyportnews.com/punews/local_story_197234849.html

5. *July 16, Reuters* — **California approves pipeline link to Mexico LNG port.** A California state commission has approved expansion of a pipeline system to bring natural gas by early 2008 into California from a liquefied natural gas (LNG) terminal off northern Mexico's Pacific coast. The North Baja Pipeline is owned by TransCanada Corp. on the U.S. side of the border, and connects with a pipeline system in Mexico owned by San Diego-based Sempra Energy. It will be part of a system that by early 2008 is to bring natural gas from Sempra's Energia Costa Azul LNG terminal near Ensenada, Baja California in Mexico to power plants primarily in northern Mexico, California, and Arizona. The move by the California State Lands Commission late on Friday, July 13, was important because it approved an environmental impact report that can be used by Riverside and Imperial county officials in California, who must also give approval, said Henry Morse, general manager of the TransCanada-owned pipeline. Morse said TransCanada hopes to get approval for its part of the pipeline system from the U.S. Federal Energy Regulatory Commission later this month. Once the Costa Azul LNG terminal opens, the North Baja Pipeline flow will be reversed to bring gas into California.

Source: [http://today.reuters.com/news/articleinvesting.aspx?type=bon dsNews&storyID=2007-07-17T020308Z_01_N16362133_RTRIDST_0 TRA NSCANADA-SEMPRA-CALIFORNIA.XML](http://today.reuters.com/news/articleinvesting.aspx?type=bon dsNews&storyID=2007-07-17T020308Z_01_N16362133_RTRIDST_0_TRA NSCANADA-SEMPRA-CALIFORNIA.XML)

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

6. *July 17, NBC 2 News (FL)* — **Chlorine gas leak sends four to the hospital.** A chlorine leak at Florida Gulf Coast University (FGCU) Aquatic Center sent four people to the hospital and left some with itchy and irritated eyes. But emergency response crews say if those people were in contact with the fumes for much longer, it could have been lethal. Officials from the FGCU Police Department say that a power outage ultimately caused bleach to leak into some hydrochloric acid which caused a chlorine gas emission. Fire crews on scene removed the harmful gas by ventilating the pool and everything has since returned back to normal.

Source: <http://www.nbc-2.com/Articles/readarticle.asp?articleid=13516&z=3&p>

7. *July 17, Associated Press* — **Factory fire leads to evacuations, warning about smoke.** A large fire at a factory that makes molds for foundries sent flames and black smoke billowing into the air Tuesday morning, July 17, prompting a few evacuations and a warning that homeowners should close their windows and doors in La Rue, OH. Authorities were concerned about the possibility of hazardous gases being released by the fire at the J-Lenco Inc. plant. Residents were advised to also bring pets indoors. After the fire was first called in around 4:45 a.m. EDT, about a dozen homes were evacuated, said Lt. Duane Meadows with the sheriff's office. By 11:30, with the fire mostly out and the smoke having cleared, those residents were allowed to return and the advisory about keeping other area homes closed up was lifted. There were no reports of injuries from the fire.

Source: <http://www.ohio.com/mld/ohio/17505043.htm>

8. *July 17, Associated Press* — **Hundreds evacuated after plant fire.** Hundreds of people were evacuated in Valley Center, KS, after an explosion Tuesday morning, July 17, at a solvents plant ignited about 660,000 pounds of chemicals, authorities said. The mandatory evacuation of the two-mile area around the plant was canceled around 10:50 a.m. CDT, but authorities weren't immediately allowing people who left their homes to return, said Andrea Anglin, a spokesperson for the Wichita chapter of the Red Cross. About 200 people had been taken to the Kansas Coliseum, about 10 miles south in Wichita. He said residents in an area a half-mile upwind and one mile downwind of the plant were still being urged to leave. People who stayed were being advised to stay on the first floor of their homes and shut off their air conditioners. Two residents in the area surrounding the plant were transported to hospitals, but the cause and extent of their injuries weren't known.

Source: http://cjonline.com/stories/071707/bre_explosion.shtml

[\[Return to top\]](#)

Defense Industrial Base Sector

9. *July 17, Federal Computer Week* — **DARPA wants better decision-making on battlefield.** The Defense Advanced Research Projects Agency (DARPA) is seeking industry proposals for a new program aimed at improving the quality and speed of decision-making for commanders on the battlefield. Dubbed "Deep Green," the project will use information technology to build what agency officials call a battle command decision support system, according to a Monday, July 16, solicitation posted on DARPA's Website. Deep Green will allow commanders to "think ahead, identify when a plan is going awry, and help develop alternatives ahead of real time," the solicitation reads. "Deep Green will ensure that the commander rarely reaches a point on the operation at which he has no options."

DARPA "Deep Green" presolicitation notice: <http://www.darpa.mil/baa/BAA07-56.html>

Source: <http://www.fcw.com/article103245-07-17-07-Web>

[\[Return to top\]](#)

Banking and Finance Sector

10. *July 18, VNUNet* — **Second-hand PCs still full of sensitive data.** Despite recent high-profile data breaches and heightened awareness of the need to delete data prior to selling a PC, many second-hand computers contain highly sensitive personal information. IT consultancy Navigant Consulting purchased three second-hand computers last week and was able to determine that one of the computers still contained sensitive personal information on its hard drive. Andrew Durant, head of Navigant's fraud investigation team, said: "The seller believed that all information had been deleted when the hard drive was reformatted and a new operating system was installed, but that is simply not good enough." Based on an analysis of the computers, Navigant fraud investigators discovered information from a community college on the second-hand computer. Data included student names, addresses and photos, staff budgets and payroll schedules including names and salary details, bank account standing data payments and receipts, and a letter including full bank account details.

Source: <http://www.vnunet.com/vnunet/news/2194451/second-hand-pcs-se nsitive>

11. *July 18, Salt Lake Tribune* — **Homeless man threatens to blow up Wells Fargo Bank building.** Police arrested a 47-year-old homeless man after he allegedly triggered a massive downtown Salt Lake City evacuation late Tuesday, July 17, by threatening to blow up a bomb in the Wells Fargo Bank building. A bomb squad robot was used to detonate a backpack police say Nicholas Dotson claimed contained an explosive device. After the bag was found only to contain clothing, a two-hour evacuation — which also shut down commuter rail traffic north of 400 South and Main Street — was ended and occupants of the 26-story Wells Fargo Building were allowed to return. Police said they do not know the man's motive; he did not appear to attempt to take hostages nor rob the bank.

Source: http://origin.sltrib.com/ci_6396553

12. *July 17, IDG News Service* — **FBI, military names being used in e-mail scams.** The FBI's Internet Crime Complaint Center (IC3) is warning of fraudulent e-mails that appear to come from the FBI and U.S. military. "The IC3 has increasingly received intelligence of fraudulent schemes misrepresenting the FBI and/or Director Robert S. Mueller III," the center said in an alert published Tuesday, July 17. "The fraudulent e-mails give the appearance of legitimacy due to the usage of pictures of the FBI Director, seal, letterhead, and/or banners." The spam is actually pumping lotteries or are phony inheritance notifications, the IC3 said. Other scams use the FBI's name to "intimidate and convince the recipient the e-mail is legitimate," the IC3 said. Criminals have used the agency's name in extortion e-mails and online auction scams as well. In a separate statement also issued Tuesday, the IC3 warned that scammers were also sending out fraudulent e-mail claiming to be from U.S. soldiers stationed overseas. "The scam e-mails vary in content; however, the general theme of each is to request personal information and/or funds from the individual receiving the e-mail," the IC3 said. The e-mails are variations on long-running scams such as the Nigerian "419" spam.

Source: http://www.infoworld.com/article/07/07/17/FBI-and-military-names-being-used-in-email-scams_1.html

13. *July 17, ComputerWorld* — **Breach, undetected since '05, exposes data on Kingston customers.** A September 2005 security breach that remained undetected until recently may have compromised the names, addresses and credit card details of roughly 27,000 online customers of computer memory vendor Kingston Technology Company Inc. The company began sending letters to affected customers informing them of the incident last week. According to a spokesperson, Kingston's IT team "detected irregularities" in the company computer systems at some unspecified point in time and — along with a team of forensic computer experts — began investigating the issues. It was not until after that probe was completed and a final report released on May 22 that Kingston could confirm the scope of the intrusion and its impact. But the company did not offer details on how or when the breach was discovered and how long it waited to notify customers about the potential compromise of data. Kingston, which had \$3 billion in sales last year, also did not offer any explanation on the nature and scope of the breach itself or why it remained undetected for so long.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027220&intsrc=hm_list

14.

July 17, InformationWeek — **McAfee quiz lets users test their phishing know-how.** McAfee SiteAdvisor, the testing and rating wing of security company McAfee, is offering a 10-question quiz to test users on how well they can avoid getting hooked into a fraudulent site that has been set up to rob them of their identifying information, as well as their money. "It's an educational campaign. It's for IT managers and the casual consumer," said Shane Keats, a research analyst with McAfee, in an interview. "Phishing cuts across all levels of technical sophistication. We all know really savvy people who have been tricked by phishing attacks because it keeps getting more sophisticated. It's harder to judge whether a site is a phishing site than you think, and frankly, we all need a little help." The quiz, according to Keats, tests people on two fronts — the psychological attack and the technical attack.

Phishing quiz: http://www.siteadvisor.com/quizzes/phishing_0707/

Source: <http://www.informationweek.com/management/showArticle.jhtml;jsessionid=Q1BN4XDCOU5IUQSNLDPCKHSCJUNN2JVN?articleID=201001810&articleID=201001810>

- 15. July 13, The Day (CT) — Pfizer waited six weeks to notify employees of data breach.** Pfizer Inc. let six weeks go by before notifying 17,000 employees and former employees that their personal information had been posted to the Internet, according to a letter from the company that state Attorney General Richard Blumenthal released Friday, July 13. Attorney Bernard Nash, in the July 11 letter, said Pfizer learned about the data breach April 18 when an independent computer services consultant informed the company about finding sensitive data on a peer-to-peer network. But Pfizer didn't start notifying the affected people until June 1, and the mailing wasn't completed until June 6, according to the eight-page letter. An investigation determined that the breach had occurred about a month earlier, on March 26, when the spouse of a Pfizer employee used a company laptop to install unauthorized software and access a file-sharing network.

Pfizer's letter: <http://media.theday.com/gbl/media/dynamic/pdfnews/webpfizerr esponse.pdf>

Source: http://www.theday.com/re.aspx?re=ccd6d003-26af-49cd-851f-a9a_c47cbe4a5

[\[Return to top\]](#)

Transportation and Border Security Sector

- 16. July 18, Associated Press — At least 195 feared dead in Brazilian jet crash.** Rescue crews pulled dozens of bodies Wednesday, July 18, from a Brazilian airliner that crashed and burst into flames at Brazil's busiest airport, as the number of people feared dead rose to 195. The TAM airlines Airbus-320 was en route to Sao Paulo from Porto Alegre in southern Brazil on Tuesday when it skidded on the rain-slicked runway in Sao Paulo, barreled across a busy road and slammed into a gas station and TAM building. On Wednesday, the airline raised the number of people aboard the plane by four to 180 and officials said the chance of anyone surviving was near zero. A Sao Paulo public safety official who spoke on condition of anonymity because of department policy said 15 bodies had been recovered from the ground. The runway at Sao Paulo's Congonhas airport has been repeatedly criticized for being too short, and two planes slipped off it in rainy weather just a day earlier, though no one was injured in either incident. There have been questions about the country's under-funded air traffic control systems, deficient radar system, and the ability to cope with a surge in travelers. Additional information on Congonhas airport:

<http://www.guardian.co.uk/brazil/story/0,,2129218,00.html>

Source: http://www.usatoday.com/news/world/2007-07-17-brazil-jet_N.htm?loc=interstitialskip

17. July 18, North Jersey Media Group — New Jersey can now track hazardous freight.

Counterterrorism investigators in New Jersey now have real-time access to information on potentially hazardous shipments on one of the nation's largest rail networks, officials said Tuesday, July 17. The map-based tracking system allows authorities to instantly locate any freight cars operated by CSX Transportation and check whether the shipment contains hazardous materials. That means they can determine vulnerabilities and shorten response time if an incident occurs. Officials herald the partnership between CSX Transportation and the homeland security offices of New Jersey and New York as the first between a private rail company and public counterterrorism agencies. Florida-based CSX Transportation, which developed the tracking system, operates 650 miles of track in New Jersey, including a line that cuts through towns such as Little Ferry, Teaneck, Dumont, and Harrington Park before crossing into New York, said company spokesperson Robert T. Sullivan. Among the country's largest rail providers, CSX Transportation transports "the lion's share" of hazardous materials, Canas said. In all, CSX operates 21,000 miles of rail in 23 states. The system is housed in New Jersey at the state police intelligence.

Source: <http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXk2MDgmZmdiZWw3Zjd2cWVIRUV5eTcxNzAxMjImeXJpcnk3ZjcxN2Y3dnFIZUVFeXky>

18. July 18, Associated Press — Experts: Runway extensions needed. On Wednesday, July 18, an international pilots association responded to the plane crash in Brazil by urging aviation authorities worldwide to install long safety strips at the end of runways to prevent routine overruns from turning into tragedies. The "tragic accident at Sao Paulo Congonhas Airport demonstrates once again the need for Runway End Safety Areas (RESA) to be established at airports with airline operations," according to a statement released by The International Federation of Airline Pilots' Associations. The British-based association, which represents 105,000 commercial pilots around the world, has been lobbying for years for all airports to be equipped with at least one 300-meter (1,000-foot) runway overrun area to allow for safer airline operations. If there is no space available to provide for safe runway extensions, airports should install soft ground beds known as the Engineered Materials Arrestor Systems that are designed to slow down planes, much as escape ramps on highways can stop trucks that lose their brakes, the association said.

Source: http://biz.yahoo.com/ap/070718/eu_plane_crash_short_runways.html?.v=2

[\[Return to top\]](#)

Postal and Shipping Sector

19. July 16, Today's Trucking — Con-way acquires Contract Freighters. One of the U.S.'s largest trucking carriers, Con-way Inc. announced it has acquired Contract Freighters Inc. (CFI), a privately held North American truckload carrier based in Joplin, MO. The acquisition, valued at \$750 million, elevates Con-way into a unique position in the freight transportation industry, creating a leading LTL, truckload (TL) and supply chain management enterprise. CFI

operates more than 2,600 tractors and over 7,000 trailers, with more than 3,000 employees, including 2,500 drivers throughout North America. CFI will be folded into Con-way's existing truckload division. Together with the complementary capabilities of LTL carrier Con-way Freight, and global supply chain services provider Menlo Logistics, the group says it will deliver an expanded transportation and logistics platform to North America-based shippers as well as global businesses, from "first-mile" sourcing in Asia or Europe, to "last-mile" delivery in North America.

Source: <http://www.todaystrucking.com/news.cfm?intDocID=18186>

20. *July 16, Newsday (NY)* — **Post office evacuated after fire.** A package on a post office conveyor belt caught fire Saturday, July 14, in Bethpage, NY, prompting an evacuation and an investigation by the Nassau police arson/bomb squad and fire marshals. A postal worker grabbed the package and put out the fire with an extinguisher. The evacuation was supervised by the Bethpage Fire Department, and the cause of the fire is being investigated by the arson/bomb squad, county fire marshal and postal service.

Source: <http://www.newsday.com/news/local/longisland/ny-lipack0717.0.5061391.story?coll=ny-linews-headlines>

[[Return to top](#)]

Agriculture Sector

21. *July 17, Agricultural Research Service* — **Gene helps explain foulbrood's spread among U.S. bees.** A gene for resistance to tetracycline drugs has been discovered in the microbe that causes the bacterial disease American foulbrood (AFB) in honey bees, according to scientists with the Agricultural Research Service (ARS). AFB, caused by the spore-forming *Paenibacillus larvae* bacterium, is so serious that infected colonies must be burned—an extremely costly option for beekeepers. From the 1950s until very recently, the only AFB treatment approved for use in the U.S. has been the antibiotic oxytetracycline (OTC), sold under the name Terramycin. But recently there have been reports of *P. larvae* suddenly developing resistance to Terramycin. ARS researchers have discovered a natural plasmid in *P. larvae*—called pMA67—that contains an OTC-resistance gene. Plasmids are small DNA molecules containing up to several dozen genes that bacteria pass on when they reproduce. This is the first report of any tetracycline-resistance gene being found in any *Paenibacillus* bacteria. In tests on 36 *P. larvae* strains gathered from across the U.S. and Canada, all 21 OTC-resistant strains were found to possess the pMA67 plasmid, and all 15 OTC-sensitive strains did not.

Source: <http://www.ars.usda.gov/is/pr/2007/070717.htm>

22. *July 17, University of Illinois* — **GPS-equipped cattle part of integrated farm system.** At a University of Illinois trust farm, the cows come equipped with GPS. It's all part of an agro-eco system that rotates corn and cattle on the same land. Scientists are analyzing this integrated system to help growers squeeze as much productivity out of their land as possible. And tracking cattle movement with GPS plays one key part in the study. This integrated farming system has been established on the Dudley Smith Farm near Pana, IL, where researchers rotate grain crops with a herd of approximately 60 beef cattle on the same land. Grain crops are grown in the summer, while cattle graze adjacent pastures. When pastures become dormant in the fall, cattle are moved to croplands, where they spend late fall and winter grazing a mixture of annual cover

crops and corn residues. In the spring, cattle are returned to the pastures.

Source: <http://www.aces.uiuc.edu/news/stories/news4075.html>

[\[Return to top\]](#)

Food Sector

23. July 17, *Animal and Plant Health Inspection Service* — USDA announces new risk-based process for certain imported fruits and vegetables. U.S. Department of Agriculture (USDA) Secretary Mike Johanns Tuesday, July 17, announced a new risk-based process for approving the importation of certain fruits and vegetables. The new risk-based process for approving certain fruits and vegetables applies only to commodities that can be imported into the U.S. subject to one or more of five designated phytosanitary measures. These measures include port-of-entry inspection, approved postharvest treatment, a phytosanitary certificate verifying that it originated from a pest-free area, a phytosanitary certificate verifying that it is free from a specified pest or pests or that the risk associated with the commodity can be mitigated through commercial practices. The importation of fruits and vegetables that require additional phytosanitary measures will continue to undergo the full rulemaking process. The changes in the rule do not alter which fruits and vegetables are currently eligible for importation or how the risks associated with those commodities are evaluated or mitigated. This rule only makes more timely the approval of fruits and vegetables that are safe for importation into the United States. USDA is also establishing a notice-based process for approving pest-free areas in exporting countries.

Source: <http://www.usda.gov/wps/portal/!ut/p/.s.7.0.A/7.0.1OB?contentonly=true&contentid=2007/07/0197.xml>

24. July 17, *Reuters* — Food safety a big problem worldwide: WHO officials. China should not be singled out for particular concern over food safety, a big problem that rich and poor countries alike must tackle through better regulation, top World Health Organization (WHO) officials said on Tuesday, July 17. Margaret Chan, WHO director-general, said the agency receives about 200 reports of tainted food products each month in its 193 member states. But many food-borne diseases go unreported and outbreaks of salmonella or E. coli bacteria can take on massive proportions according to the WHO. The WHO issues about 10 to 20 "emergency notifications" each year, signaling a potential international public health problem linked to food.

Source: <http://www.reuters.com/article/healthNews/idUSL171562120070717>

25. July 17, *Associated Press* — Congress: FDA lab closure plan too risky. Importers have learned to evade close federal scrutiny of the food they ship into the U.S., congressional investigators said Tuesday, July 17. Lawmakers also criticized the U.S. Food and Drug Administration's (FDA) plan to close half of its laboratories. They called that idea misguided. The FDA's ability to police the nation's food supply has come under criticism from Congress and others amid a string of high-profile cases of foodborne illness. FDA commissioner Andrew von Eschenbach said the lab plan was meant to modernize the FDA's food safety efforts. An Energy and Commerce Committee investigation found the FDA now has little ability to police imports. In San Francisco, for example, the FDA's staff can conduct only a cursory review of imports, generally dedicating just 30 seconds to each shipment as it flashes by on a computer

screen, according to investigators. Even when products are flagged by the FDA, importers have learned to game the system, investigators said. For example, the FDA relies on results obtained from private labs before clearing and releasing suspect imports. Those results are driven by financial rather than scientific concerns, investigators told the subcommittee.

Source: <http://www.forbes.com/feeds/ap/2007/07/17/ap3922879.html>

26. July 16, *Chicago Tribune* — Food safety lacks teeth, critics say. The makers of Veggie Booty, a snack food recalled from stores late last month, weren't sure what was wrong with their product, according to federal food safety officials. All they knew was that officials at the U.S. Centers for Disease Control and Prevention (CDC) were telling them that people had eaten Veggie Booty and fallen ill, eventually 61 sickened in 19 states. That confusion points up just how cumbersome the nation's food recall procedures can be, both for consumers and companies. Under the current system, the federal agencies responsible for food safety can't actually force companies to issue recalls. And when recalls do occur, just a fraction of the tainted food is ever recovered. Veggie Booty's maker, recalled its product at the suggestion of the U.S. Food and Drug Administration (FDA). But neither the CDC nor FDA ever discovered on their own just what was wrong with Veggie Booty. That answer came from the Minnesota Department of Agriculture, which took it upon itself to test suspect bags of Veggie Booty. It informed the manufacturer of its findings: Salmonella Wandsworth.

Source: http://www.chicagotribune.com/news/nationworld/chi-recall_hedges_16jul16.1.5169638.story?coll=chi-newsnationworld-hed

[\[Return to top\]](#)

Water Sector

27. July 18, *Associated Press* — European Union calls for pay-as-you-use water pricing.

Europeans should pay for water as they use it — rather than forking out a one-time user fee — to encourage efficiency and help stave off water scarcity and droughts, the European Union (EU) said Wednesday, July 18. Faced with the prospect of inadequate water resources in the future, the EU's executive commission suggested the EU's 27 member states implement a "user pays" principle and promote the installation of water-saving devices on household taps, shower heads and toilets. These recommendations were adopted by the EU more than seven years ago but many member states have not implemented efficiency pricing programs. The cost of droughts to the EU economy over the past 30 years was at least \$138 billion, the EU said. A widespread drought in 2003 — which affected over 100 million people and about a third of EU land area — cost approximately \$12 billion.

Source: <http://www.iht.com/articles/ap/2007/07/18/europe/EU-GEN-EU-Water-Scarcity.php>

28. July 17, *Reuters* — New China algae outbreak threatens water supplies. An outbreak of blue algae in a Chinese reservoir has left nearly 25,000 people without water and 100,000 others with reduced supplies, state media said on Wednesday, July 18. The local government had started collecting the algae using nets and boats and was trucking in water to residents in Changchun's Luyuan district where supplies have been suspended. Water supplies to millions of residents have been affected in a series of algae outbreaks across the country in recent months. On July 4, water supplies to 200,000 people in Shuyang county were halted for more than 40 hours after ammonia and nitrogen were found in a local river. In late May, a major

outbreak in China's third biggest lake cut off water supplies to over two million residents of Wuxi city.

Source: http://www.reuters.com/article/healthNews/idUSPEK15919320070_718

[\[Return to top\]](#)

Public Health Sector

29. July 17, *Associated Press* — TB patient who fled Arkansas hospital found. A man with tuberculosis (TB) who fled from medical isolation at a hospital was found Tuesday, July 17, near Little Rock, AR, authorities said. Pulaski County Sheriff's spokesperson John Rehrauer said Franklin Greenwood was being taken back to the University of Arkansas for Medical Sciences hospital. A district judge had ordered Greenwood placed in isolation on June 29 after he was seen coughing up blood outside of the city's traffic court. Greenwood fled on July 1. Health officials said Greenwood is contagious but has a form of TB that can be controlled with treatment. They don't believe his TB is drug-resistant, but they want to test him further to determine if he is a safety risk.

Source: <http://www.signonsandiego.com/news/nation/20070717-0903-tbqu-arantine.html>

30. July 17, *CIDRAP News* — White House issues one-year status report on pandemic planning. The White House Homeland Security Council Tuesday, July 17, released a one-year update on the federal government's pandemic influenza preparedness strategy, reporting that it has met 86 percent of the objectives it set for itself a year ago. Work on the remaining 14 percent of the actions is in progress and should be completed by the 18-month mark. The U.S. government has provided H5N1 surveillance and response training to more than 129,000 animal health workers and 17,000 healthcare workers worldwide. The U.S. has donated 300,000 personal protective equipment kits to surveillance and outbreak response workers in more than 70 countries, and it has prepositioned overseas stocks of protective supplies, decontamination kits, and antiviral medication. In the past year, the U.S. has invested more than one billion dollars to develop new vaccine technologies. The Food and Drug Administration (FDA) approved the first pre-pandemic H5N1 vaccine, and federal officials have stockpiled enough doses to treat six million people. The government has invested \$600 million for state and local preparedness efforts, which support the development of community mitigation strategies, medical surge plans, and mass vaccination strategies. The government says it has launched new guidelines to improve emergency medical service delivery and 911 service in a pandemic setting.

Report: <http://www.whitehouse.gov/homeland/pandemic-influenza-oneyear.html>

Source: <http://www.cidrap.umn.edu/cidrap/content/influenza/panflu/news/jul1707whitehouse.html>

31. July 17, *U.S. Department of Health and Human Services* — HHS announces funding to states for public health preparedness and emergency response. U.S. Department of Health and Human Services (HHS) Secretary Mike Leavitt Tuesday, July 17, announced that the department has provided another \$896.7 million to the states, territories, and four metropolitan areas to improve and sustain their ability to respond to public health emergencies. HHS' Centers for Disease Control and Prevention (CDC) is coordinating the funding to be used for preparedness and response to all-hazards public health emergencies including terrorism,

pandemic influenza, and other naturally-occurring public health emergencies. The funding includes: \$175 million for pandemic influenza preparedness to assist public health departments in their pandemic influenza planning efforts; \$57.3 million to support the Cities Readiness Initiative (CRI); \$35 million to improve the early detection, surveillance, and investigative capabilities of poison control centers to provide information to health care providers and the public to respond to chemical, biological, radiological, and nuclear events; and \$5.4 million is specifically allocated for states bordering Mexico and Canada for the development and implementation of a program to provide effective detection, investigation, and reporting of urgent infectious disease cases in the three nations' shared border regions.

Source: <http://www.hhs.gov/news/press/2007pres/07/pr20070717c.html>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

32. *July 17, Federal Emergency Management Agency* — President declares major disaster for North Dakota. The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced that federal disaster aid has been made available for North Dakota to supplement state and local recovery efforts in the area struck by severe storms and flooding during the period of June 2–18, 2007. FEMA Administrator David Paulison said federal funding is available to state and eligible local governments and certain private nonprofit organizations on a cost-sharing basis for emergency work and the repair or replacement of facilities damaged by the severe storms and flooding. Areas covered by the declaration include Barnes, Bowman, Dickey, Grant, LaMoure, Logan, McHenry, Ransom, Richland, Sargent, and Stutsman counties.

Source: <http://www.fema.gov/news/newsrelease.fema?id=37890>

33. *July 17, Resident Publications (NY)* — In disaster aid, scientists look to bugs to help rescuers communicate. During the tsunami in South Asia, hurricanes in Florida, earthquakes in Iran, and the 9/11 terrorist attacks, rescuers encountered the same challenge: how to communicate with each other amid the chaos. Reports after each crisis showed that rescue coordinators were often overwhelmed by the sheer scale and complexity of the efforts. Vital information didn't reach the right people. Faced with this problem, where can rescuers turn for help? To nature itself, suggests a team of nine researchers at the University of Illinois at Urbana-Champaign. The group, whose expertise spans computer science, psychology, linguistics, neuroscience and civil engineering, recently received \$2.37 million from the National Science Foundation to study the behavior of honeybees, ants and viruses. These creatures produce complex, surprisingly effective patterns of communication. By combining their own observations with those of others in the field, the researchers plan to use the organisms' natural networks as models for software that would run on handheld computers.

Source: <http://70.47.124.114/node/779>

Information Technology and Telecommunications Sector

34. July 18, Sophos — **Sophos reveals top 12 spam-relaying countries.** Sophos has published its latest report on the top twelve spam-relaying countries over the second quarter of 2007. The U.S. continues to relay more spam than any other nation, accounting for 19.6 percent — a decrease of just 0.2 percent from the previous quarter. However, Europe now has six entries in the top 12 spam-relaying countries list, which when combined, account for even more spam-relaying than the U.S. Sophos notes that the number of compromised PCs continues to rise steadily in Europe. The top twelve spam-relaying countries are as follows: 1) United States; 2) China (including Hong Kong); 3) South Korea; 4) Poland; 5) Germany; 6) Brazil; 7) France; 8) Russia; 9) Turkey; 10) United Kingdom; 10) Italy; 12) India.

Source: http://www.sophos.com/pressoffice/news/articles/2007/07/dirt_ydozjul07.html

35. July 18, Reuters — **China Internet censors blamed for e-mail chaos.** Internet users and company officials in China on Wednesday, July 18, blamed a series of disruptions to cross-border e-mail traffic on adjustments to the country's vast Internet surveillance system. IT company executives offered varying explanations for the e-mail disruptions, but agreed they were not a result of standard technical problems. China is in the midst of a highly publicized campaign to rein in "unhealthy content" in its rapidly growing Internet, whose rapid spread of information regarding incidents of government corruption and rural unrest not reported in conventional media has alarmed China's stability-obsessed leaders. "We have had hundreds of complaints from our clients in the last couple of days," said Richard Ford, technical director of Candis Group, a Beijing-based IT company that processes hundreds of thousands of e-mails a day. Ford said clients complained of e-mails being returned with error messages that could only have been placed by a "third party" between local and foreign mail servers. Several other IT companies managing e-mail servers confirmed Internet users and clients in China and overseas had complained of having trouble sending and receiving e-mails.

Source: <http://www.informationweek.com/security/showArticle.jhtml;jsessionid=KZVNFLPTIUFBWQSNDLOSKHSCJUNN2JVN?articleID=201001971&articleID=201001971>

36. July 17, eWeek — **Oracle update plugs security holes.** Oracle issued 45 security fixes for its customers Tuesday, July 17, as part of its quarterly Critical Patch Update. The 45 patches plug security holes in Oracle Database, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and Applications, and Oracle PeopleSoft Enterprise products. The most serious of the flaws are two vulnerabilities affecting Oracle PeopleSoft Enterprise PeopleTools and received a Common Vulnerability Scoring System rating of 4.8 out of 10. The flaw can be exploited remotely by attacker but requires user authentication.

Oracle Critical Patch Update: <http://www.oracle.com/technology/dep/technology/critical-patch-updates/cpujul2007.html>

Source: <http://www.eweek.com/article2/0,1895,2159759,00.asp>

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

37. *July 17, Record-Courier (NV)* — Suspects experimenting with pipe bombs cause fire.

Douglas County, NV, officials are investigating a one-acre fire Saturday night, July 14, in Wellington they believe was started by suspects experimenting with pipe bombs and other incendiary materials. East Fork Fire Capt. Terry Taylor said Tuesday the fire was ruled third-degree arson, a felony offense. “It was willfully and maliciously set by human beings and primarily burning in vegetation,” he said. In addition to county law, the suspects would be in violation of federal law because the fire was on Bureau of Land Management land. “They had constructed a variety of explosive and incendiary devices and also had components for additional incendiary devices,” Taylor said. “At some point, they detonated at least one of the explosive devices.”

Source: <http://www.recordcourier.com/article/20070717/NEWS/70717009>

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.